WHAT IS CLAIMED IS:

A1. A system for authenticating a user, the system comprising:

a sending system connected to a network and comprising a processor connected to a storage device, one or more input/output devices, and a port for communicating through the network wherein the processor is configured to send a digital certificate, a password associated with a user identity, and a hardware identifier that is associated with the sending system over the network to a server system and to execute software using a secure layer protocol located between an application layer and a transport layer, and

the server system connected to the network to receive the digital certificate, a password associated with a user identity, and a hardware identifier, the server system comprising a processor configured to execute software located between the application layer and the transport layer capable of authenticating, based on the received digital certificate and the received password, a user identity of the sending system and authenticating, based on the received the hardware identifier, the sending system.

2. The system of claim 1 wherein:

the processor of the sending system is further configured to send a public key over the network to the server system, and

the processor of the server system is further configured to receive the public key and the executing software is further capable of authenticating the user identify of the sending system based on both the received digital certificate and the received public key.

3. The system of claim 1 wherein the server system is further configured to:

determine permitted access to content associated with the server system; and

allow only permitted access to the content associated with the server system.

4. The system of claim 1 wherein the server system is further comprised of multiple servers and one or more processors of the server system are further configured to perform load balancing of network connection requests across the multiple servers.

5. The system of claim 1 wherein:

the sending system is further configured to create a digital signature associated with a hardware component of the sending system,

the processor of the sending system is further configured to:

encrypt a hardware identifier, and

send the encrypted hardware identifier to the server system, and

the server system is further configured to receive and store the hardware identifier for use in authenticating the hardware of the sending system.

6. The system of claim 5 wherein the sending system is configured to generate the hardware identifier.

7. The system of claim 5 wherein the server system is configured to generate the hardware identifier and send the hardware identifier to the sending system.

B1. An authentication proxy server connected to a network, the authentication proxy server comprising a processor connected to a storage device, one or more input/output devices, and a port for communicating through the network wherein the processor is configured to receive a digital certificate, a password associated with a user identity, and a hardware identifier, and execute software logically operating between an application layer and a transport layer of a communications protocol stack for the purpose of authenticating, based on the received digital certificate and the received password, a user identity of a client system associated with the digital certificate and password, and authenticating, based on the received the hardware identifier, the client system.

B2. The authentication proxy server of claim B1 wherein:

digital certificate includes an identification of the certificate authority that issued the digital certificate and a public key of a sending system associated with the digital certificate such that the public key has been encrypted with the private key of the certificate authority, and

the processor is further configured to execute software logically operating between the application layer and the transport layer:

receive a public key of a sending system associated with the digital certificate,

use the public key of the certificate authority to decrypt the public key of the sending system included in the digital certificate, and

authenticate the user identity when the decrypted public key corresponds to the received public key.

C1. A client software application that communicates with the authentication proxy server of claim B1 wherein:

client software application provides a specialized communication protocol for communicating with the authentication proxy server

client software application provides a specialized authentication protocol for authenticating with the authentication proxy server

client software application provides a specialized security protocol for encrypting and decrypting communication data with the authentication proxy server.

C2. The system of claim C1 wherein:

the client software application contains an hypertext markup rendering module that will display decrypted data from the authentication proxy in a secure fashion, preventing user access to the data in any manner other than through the rendered display.